Қазақстан Республикасы Тәуелсіздігінің 30 жылдығына арналған «Сейфуллин оқулары – 17: «Қазіргі аграрлық ғылым: цифрлық трансформация» атты халықаралық ғылыми – тәжірибелік конференцияға материалдар = Материалы международной научно – теоретической конференции «Сейфуллинские чтения – 17: «Современная аграрная наука: цифровая трансформация», посвященной 30 – летию Независимости Республики Казахстан.- 2021.- Т.1, Ч.3 - С. 79 - 82

LOCAL NETWORK RESEARCH AND DATA TRANSFER ANALYSIS IN THE GNS3 EMULATOR

Karpenko M.S.,
Kismanova A.A.

The article studies and builds a local network in the GNS3 program emulator , and also uses the Wairshark program for traffic analysis and packet capture . This article allows us to conclude that the packets that are sent over the network can be encrypted, and can be in the public domain. In this article, we will look at two types of protocol. One protocol encrypts the information, and the other protocol sends the information in an open form.

The purpose of this article is to study the local network in the GNS3 program and to study data transmission over two protocols.

Keywords: GNS3 program emulator, SSH protocol, TELNET protocol, dynamic DHCP protocol, ICMP protocol.

Currently, many programs are used to study local and global networks, but many users are used to working on the Microsoft Windows operating system, and for this, to analyze traffic and ensure a secure Internet connection in any organization, they used the GNS3 program. In addition, the Wairshark traffic analyzer program is included in the build for this program, it will show us sending packets in open and encrypted form.

The relevance of this article is to compare the two Internet protocols and which protocol is better to use for remote access to ensure the security of data transmission .

In this example, we will only talk about two data transfer protocols,

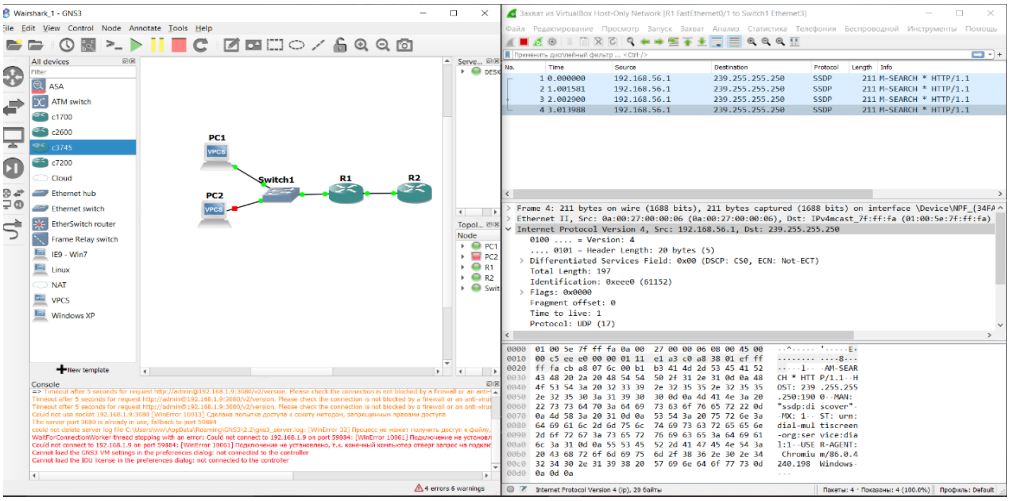
and we will also consider the speed at which data is transmitted, and the size of the packet. And what protocols does the local Internet network use?

In the current version, the GNS3 environment uses the following software for its operation: - WinPcap-system driver and function library. You can use the Wairshark program to analyze traffic and capture packets The multiservice network topology is created on the GNS3 software platform ICMP,TCP, DHCP,TELNET, SSH Protocols are used in the Wairshark program on the GNS3 emulator ICMP-ICMP can be used with both IPv4 and IPv6. ICMPv4 is a messaging protocol for IPv4. The ICMPv6 protocol provides the same services for IPv6, but it also includes additional functionality. In this course, the term ICMP

will be used to refer to both ICMPv4 and ICMPv6.[2] There are many types of ICMP messages and the reasons for sending to ICMPv4 and ICMPv6 and discussed in this module include:

- The reachability of a host;
- The destination node or service is unavailable;
- Timed out.

- In larger networks, as well as in networks with frequently changing users, it is preferable to assign addresses using DHCP. There may be new users who need to connect to the network. And other users can install new computers that also require a connection. Instead of using static addressing for each connection, it is much more efficient to automatically assign IPv4 addresses.(picture 1.1, 1.2).



Picture 1.1 Network traffic analysis of a multiservice network

Begin with, we will configure the ip address on the R1 interface , give it the address 192.168.1.1 and the mask /24 bit 255.255.255.0 After this operation, we configure the dynamic routing protocol on R1 DHCP. [7]

R1(if-config)# interface f 1/0 ip address 192.168.1.1 255.255.255.0

R1(if-config)# no shutdown

After that, we configure the dns server 8.8.8.8, Go to the computer and send a request to the DHCP server and the server gives the address 192.168.1.2 mask 255.255.255.0 and Gateway 192.168.1.1

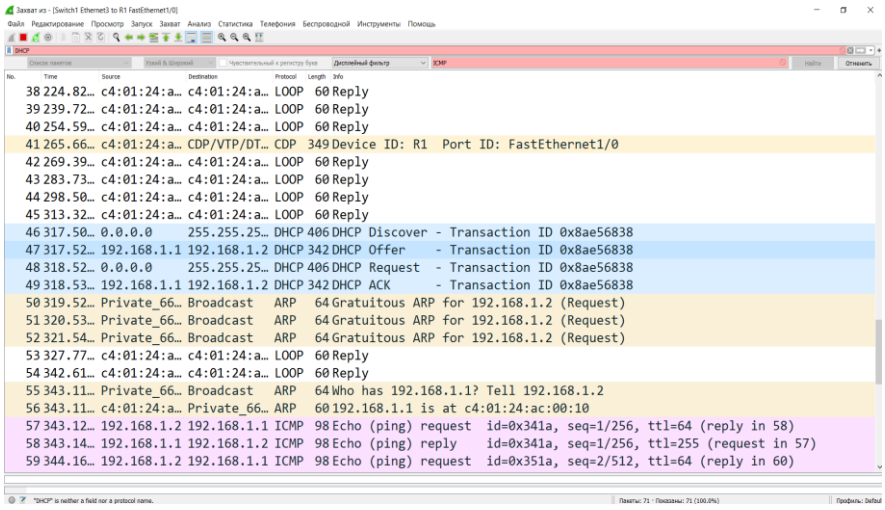
ip dhcp pool TEST

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 8.8.8.8

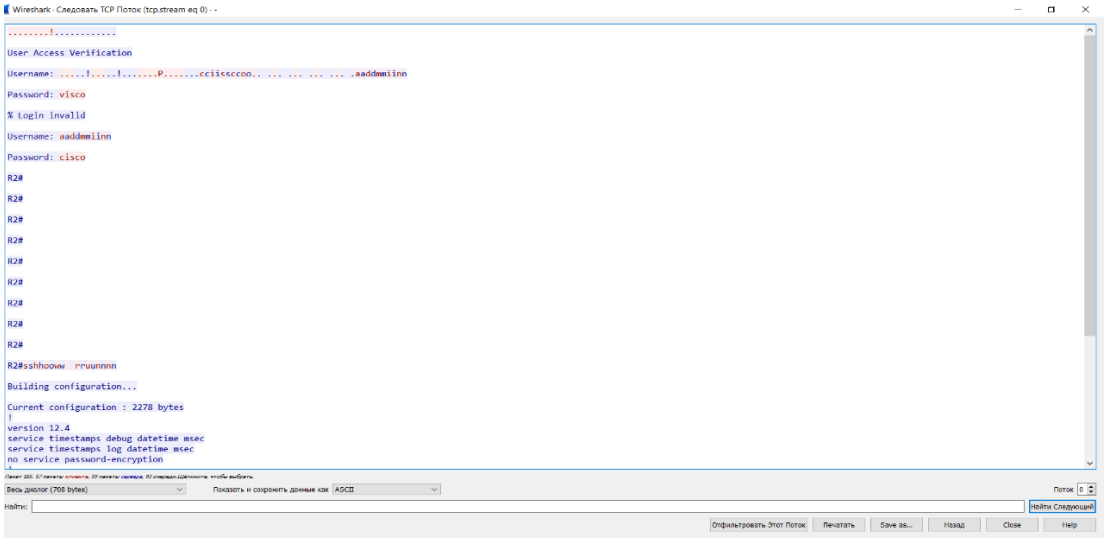
Next we analyze the traffic using the Wireshark program go to the GNS3 program click start capture after that we see which packet are coming and which are being sent And what protocol is used in this case? we use the protocol of DHCP an ICMP .(show on the picture 1.1 and 1.2)



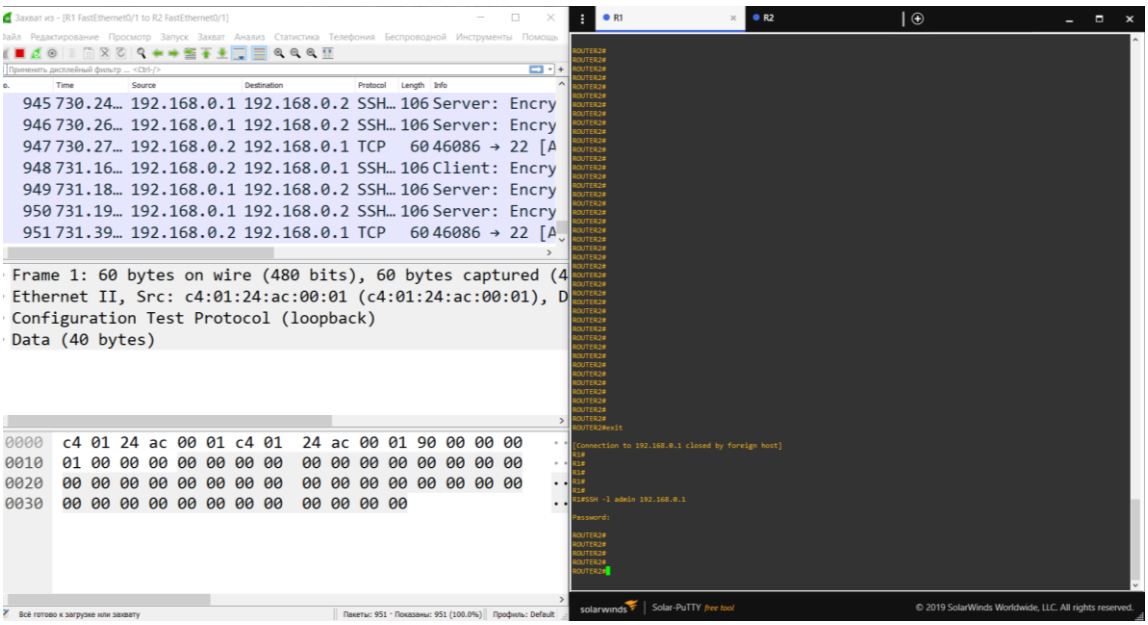
Picture 1.2 send DHCP protocols

Next, we set up remote access to R2 under the name Telnet and analyze the traffic coming to R1 in the clear nothing is encrypted, then we set up remote access toR2 SSH and the incoming traffic to R1 was encrypted.

Open TELNET traffic in the figure we can see that the PASSWORD an the USER are visible (show on the picture 1.3)

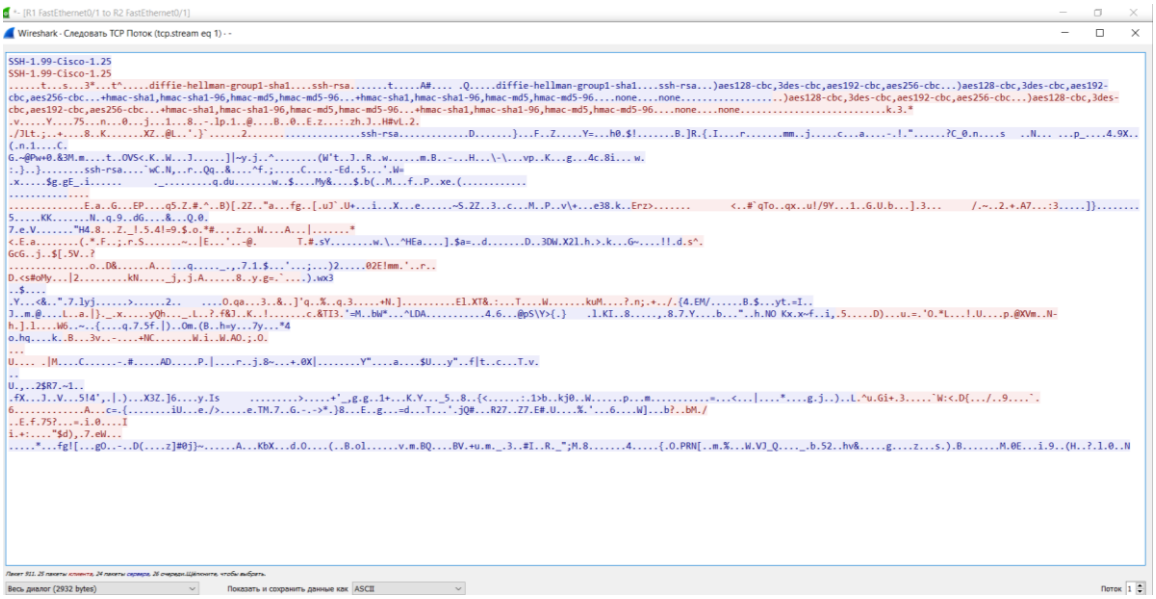


Picture 1.3 Open protocol TELNET



Picture 1.4 Encrypted protocol SSH

In this picture, we can see that the traffic is encrypted via SSH 256 characters 1024 bytes.(show on the picture 1.5)



Picture 1.5 256 characters 1024 bytes

In this work, two protocols were considered in open and encrypted form, and the DHCP protocol was also configured, which makes it possible to get an ip address automatically.

In conclusion, we can say that two protocols have been investigated, it can be seen that the Telnet protocol sends data in clear text, and the Ssh protocol encrypts this data in the sha 256 character format of the md 5 encryption format.

List of references

1.Introduction to Networks Course (netacad.com)- Cisco introduction to networks.p1.2019г.

2.GNS3 Network Simulation Guide – authors Chris Welsh.p-35.2013г.

3.Wireshark & Ethereal Network Protocol Analyzer Toolkit.-author Andrew Williams.- p25.2017г

4.www.cdo.keu.kz – Programms networks technologies . author Ten Tatiana.p 4-5.2019г.

5.Author В.Олифер, Н.Олифер.-“PC networks. Principles of technology, protocols. - p-32.2016.

6.Э. Tannenbaum, Д. Uezeroll "PC networks" 5-th edition.p-25.(2016)

7.D.Krouz, T.Ross “Computer networks”p-35.2016

8.A.Robachevskiy “Internet from the inside . Ecosystem global networks ”p-25.2017г.

9.A.Sergeev “ Fundamentals of Local computer networks ”p-23.2016г.

10.“PC networks. 5th editions” Tannenbaun Endrue, Uezeroll David .p-32.2015г.